приложения. Основа безопасности сетей мониторинга — центр управления безопасностью, который на этапе конфигурирования сети управляет подключением устройств, а также обеспечивает обновление в процессе сбора данных ключей сети.

В сетях ZigBee предусмотрено три типа ключей для управления безопасностью. Первоначальный главный ключ должен быть получен через безопасную среду (передачей или предварительной установкой), так как безопасность всей сети зависит от него. Он не используется для шифрования и применяется как разделяемый двумя устройствами секретный код при выполнении устройствами процедуры генерации ключа канала связи. Сетевые ключи обеспечивают безопасность сетевого уровня, и такой ключ имеет каждое устройство в сети ZigBee. По беспроводным каналам сетевые ключи должны пересылаться только в зашифрованном виде. Ключи каналов связи обеспечивают безопасную одноадресную передачу сообщений между двумя устройствами на уровне приложений.

НЕЛИНЕЙНЫЕ МНОЖЕСТВА КОДОВЫХ СЛОВ

А.И. Митюхин, Р.П. Гришель

В специальных системах одним из основных требованием является структурная защита информации от несанкционированного доступа к ней. Определенная степень структурной защиты обеспечивается при использовании сравнительно большого, меняющегося со временем, ортогональных и биортогональных последовательностей с кодовым расстоянием $d=n/2$, где n — длина кода.[1]. В работе рассматривается нелинейная кодовая конструкция. Она позволяет создать усеченное нелинейное множество последовательностей вида $a=(a_1, a_2, \ldots, a_{2l})$, а $\in 1, -1$, l —нечетные числа с $d'>d$. Все множество образуется диадными перестановками образующей последовательности, получаемой мажоритарным суммированием ортогональных функций Радемахера с кратным периодом. Приводятся результаты численного исследования корреляционных спектров последовательностей. Выяснено, что математическое ожидание и дисперсия корреляционных выбросов зависит от длины последовательностей. Исследовалась усеченная нелинейная кодовая конструкция кода длиной $n=32$ с минимальным расстоянием Хэмминга $d=12$ на множестве с явно выраженными спектральными компонентами. Корректирующая способность кода $t=5$. На основе анализа спектральной и структурной регулярности корреляционных спектров мажоритарных последовательностей удалось сформировать конструкции из 120 множеств нелинейных последовательностей, состоящих из четырех слов с расстоянием $d=20$.

Литература

1. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки: пер. с англ. М., 1979.

ЗАЩИТА КОРПОРАТИВНЫХ СЕТЕЙ СВЯЗИ ОТ ВНЕШНИХ АТАК

Н.А. Павлов

Одной из самых актуальных задач в сфере услуг предоставления информации является борьба с DDoS-атаками.

Для повышения качества фильтрации трафика в корпоративной сети компании от нежелательной нагрузки был разработан модуль обработки внешних запросов и внедрена система автоматического обнаружения DDoS атак в телекоммуникационной корпоративной сети и усовершенствованы алгоритмы фильтрации.

Данный модуль представляет собой защиту от DDoS атак методом HTTP флуда посредством внедрения специализированного программного кода в тело сайта, которое будет отвечать на первоначальные атаки. Данный модуль работает как быстрый фильтр между ботами и бэкэндом во время L7 DDoS атаки и позволяет отсеивать мусорные запросы, при высоких нагрузках будет передавать защиту как эстафетную палочку на следующий уровень защиты.

Разработанный модуль хорошо применять в случае связки с более производительным и дорогостоящим оборудованием, которому будут передавать информацию об активности на том или ином ресурсе.

В ходе работы были усовершенствованы системы безопасности магистральных провайдеров связи от DDoSатак. Предложенный алгоритм настройки сетевого оборудования провайдеров уровня Tier 2-3 обеспечивает быстрое взаимодействие в блокировке атакующих сетей от DDoSатак, а также позволяет проактивно реагировать на изменения в сетевой активноти.

В результате компания получила усовершенствованную магистральную сеть между центрами обработки данных с повышенным уровнем доступности, экономей входящего-исходящего трафика за счет сокращения DDoS атак, высоким уровнем утилизации оборудования за счет своевременного прекращения обработки вредоносного трафика, а также автоматизация работы с приложениями оповещения угроз, и существенное сокращение временных издержек на поиски решений и отражения DDoS атак.

Литература

1. Abliz M. Internet Denial of Service Attacks and Defense // Pittsburgh: University of Pittsburgh Technical Report [Электронныйресурс]. – Режимдоступа: http://www.cs.pitt.edu/

2. Приходько Т.А. Исследование вопросов безопасности локальных сетей на канальном уровне модели OSI [Электронный ресурс]. – Режим доступа: http://ea.donntu.org/

МОДУЛЯЦИЯ ПОЛОЖЕНИЕМ ИМПУЛЬСА В РАДИО ИДЕНТИФИКАТОРАХ ОБЪЕКТОВ

В.Т. Першин, А.Р. Буренков

Весьма перспективным в настоящее время, является использование модуляции положением импульса (Pulse Position Modulation, PPM) в радио идентификаторах объектов, представляющей собою инструмент технологии сверхширокополосной связи (Ultra Wide Band, UWB), идея которой заключается в использовании сверхширокополосного сигнала для передачи информации. В докладе представлены результаты исследования реализации метода PPM для повышения скрытности работы системы с радиочастотными идентификаторами объектов.

По виду воздействия на исходную информацию такой подход заменяет методы криптографического преобразования. Для традиционных средств связи сигналы UWB с PPM не доступны не только к приему, но даже и к определению самого факта своего существования. Поэтому модуляция положением импульса упрощает решение задачи повышения скрытности исходной информации от искажения или подслушивания ее несанкционированным пользователем. Кроме того, важно отметить, что организация криптографического процесса представляет собой значительный объем работы по выполнению многочисленных операций.

Длительность излучаемого моноимпульса может колебаться в пределах 0,2 – 2 нс, а период импульсной последовательности составляет от 10 до 1000 нс. Главные параметры, характеризующие UWB-устройства, – частота повторения коротких импульсов, средняя мощность в пересчете на 1 МГц и пиковая мощность в любой полосе шириной не менее 500 МГц. Важна также относительная ширина полосы, определяемая как отношение необходимой ширины полосы к значению центральной частоты (предполагается, что типичное значение этого параметра должно превышать 0,2).

Образование ряда независимых каналов связи может осуществляться методом временных перескоков, основанном на вводе еще одного дополнительного временного кодирования положения импульсов с помощью последовательности псевдослучайных кодов, обеспечивающих сдвиг импульсов на величины в 10 – 100 раз большие, чем дает модуляция передаваемыми данными. Для выделения сигнала в приемной части должна использоваться такая же последовательность псевдослучайных кодов. В случае применения иной